#13

PATENT
3782-0113P

IN THE U.S. PATENT AND TRADEMARK OFFICE

Applicant:	Christer FAHRAEUS et al.	Conf.:	8101
Appl. No.:	09/813,115	Group:	2161
Filed:	March 21, 2001	Examiner:	
For:	SECURED ACCESS USING A COORDINATE SYSTEM		

L E T T E R

Assistant Commissioner for Patents
Washington, DC 20231

July 23, 2001

Sir:

Under the provisions of 35 U.S.C. § 119 and 37 C.F.R. § 1.55(a), the applicant(s) hereby claim(s) the right of priority based on the following application(s):

Country	Application No.	Filed
SWEDEN	0000942-3	March 21, 2000

A certified copy of the above-noted application(s) is(are) attached hereto.

If necessary, the Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 02-2448 for any additional fee required under 37 C.F.R. §§ 1.16 or 1.17; particularly, extension of time fees.

Respectfully submitted,

BIRCH, STEWART, KOLASCH & BIRCH, LLP

By Charles Gorenstein #32924
Michael K. Mutter, #29,680

P.O. Box 747
Falls Church, VA 22040-0747
(703) 205-8000

MKM/jdj
3782-0113P

Attachment

(Rev. 01/22/01)

3782-0113P
09/813,115
3/21/01
Christer FAHRAEUS et al.
BSKB
703-205-8000

PRV

PATENT- OCH REGISTRERINGSVERKET
Patentavdelningen

Intyg
Certificate

Härmed intygas att bifogade kopior överensstämmer med de handlingar som ursprungligen ingivits till Patent- och registreringsverket i nedannämnda ansökan.

This is to certify that the annexed is a true copy of the documents as originally filed with the Patent- and Registration Office in connection with the following patent application.

(71) *Sökande* Anoto AB, Lund SE
Applicant (s)

(21) *Patentansökningsnummer* 0000942-3
Patent application number

(86) *Ingivningsdatum* 2000-03-21
Date of filing

Stockholm, 2001-03-19

För Patent- och registreringsverket
For the Patent- and Registration Office

Hjördis Segerlund

Hjördis Segerlund

Avgift
Fee 170:-

CERTIFIED COPY OF PRIORITY DOCUMENT

PATENT- OCH REGISTRERINGSVERKET
SWEDEN

Postadress/Adress
Box 5055
S-102 42 STOCKHOLM

Telefon/Phone
+46 8 782 25 00
Vx 08-782 25 00

Telex
17978
PATOREG S

Telefax
+46 8 666 02 86
08-666 02 86

AWAPATENT AB
Kontor/Handläggare
Malmö/Gunilla Larsson

ICONIZER AB
Ansökningsnr

Vår referens
SE-2000875

INLOGGNING

Tekniskt område

Föreliggande uppfinning avser ett system för styrning av en användares åtkomst av en åtkomstskyddad enhet, en kontrollanordning för kontroll av en användares åtkomst av en åtkomstskyddad enhet, ett sätt att styra åtkomst, ett datorprogram för åstadkommande av sättet och en användning av ett positionskodningsmönster.

Bakgrundsteknik

För att skydda olika typer av system och anordningar, såsom exempelvis datorer eller annan elektronisk utrustning, från obehöriga personer är det känt att utrusta dem med någon typ av åtkomstskydd. Ett vanligt åtkomstskydd för en dator består i att en användare måste logga in på datorn för att kunna använda den. Vid inloggningen matar användaren in sin användaridentitet och ett lösenord till datorn som kontrollerar dessa uppgifter mot tidigare lagrade uppgifter för att bestämma om användaren är behörig att använda datorn. Nackdelen med detta förfarande är att en användare måste memorera sitt lösenord, vilket kan vara svårt då vi omger oss med många system som kräver inloggningsförfarande, och då dessa ofta har olika lösenord. Många skriver ner sina lösenord, med följden att om någon hittar noteringen kan denna person enkelt ta sig in i det till lösenordet hörande systemet. Har användaren då också samma lösenord till flera olika system kan detta få långtgående konsekvenser.

I den japanska skriften JP10222241 "Electronic pen, and system and method for individual authentication" beskrivs en elektronisk penna som är utrustad med en gyrosensor, som när användaren skriver sin signatur med pennan, känner av sårdrag i signaturen och gör med en algoritm om dessa till ett lösenord.

Det är vidare känt genom WO 99/48268 att ersätta PIN-koden i en mobil kommunikationsenhet med en signatur som användaren skriver med kommunikationsenheten. Kommunikationsenheten är utrustad med en sensor, av typ gyrosensor eller tryckkula, som känner av rörelsen då användaren skriver med enheten.

Ett problem med ovan nämnda tekniker är att en signatur inte är speciellt svår att förfalska.

Sammanfattning av uppfinningen

Ett ändamål med uppfinningen är därför att åstadkomma ett system som möjliggör enkel och säker styrning av åtkomsten till en åtkomstskyddad enhet.

Detta ändamål uppnås med ett system enligt krav 1, en kontrollanordning enligt krav 13, ett sätt enligt krav 23, ett datorprogram enligt krav 30 och en användning enligt krav 31.

Närmare bestämt avser uppfinningen enligt en första aspekt ett system för styrning av en användares åtkomst av en åtkomstskyddad enhet, varvid systemet innefattar en användarenhet, som är anordnad att registrera minst två koordinater, och kontrollorgan, som är anordnade att, på basis av nämnda två koordinater, kontrollera om användaren är behörig att komma åt den åtkomstskyddade enheten och att om så är fallet avge en klarsignal till den åtkomstskyddade enheten.

Uppfinningen bygger på idén att använda en ny parameter, nämligen koordinater, som grund för styrningen av åtkomst till en åtkomstskyddad enhet. En fördel med ett system som är baserat på koordinater är att det, såsom kommer att framgå nedan, kan utformas med varierande grad av säkerhet, allt från mycket enkla system där det räcker att registrera ett korrekt koordinatpar till mycket säkra system där både exempelvis ett korrekt koordinatpar och en korrekt signatur och/eller användarenhetsidentitet måste registreras.

Koordinater är speciellt lämpade att använda som bas för åtkomststyrning när den åtkomstskyddade enheten sak-

nar tangentbord, eftersom koordinater kan registreras exempelvis genom en avläsning med en sensor.

Koordinaterna kan exempelvis med fördel registreras genom att användarenheten optiskt avläser ett positionskodningsmönster som kodar koordinater för ett flertal punkter. Åtkomst till en åtkomstskyddad enhet kan då göras beroende av att användaren registrerar koordinater för punkter inom ett bestämt koordinatområde.

Koordinater är också speciellt lämpade att användas som parameter för åtkomststyrning i system för elektronisk registrering av handskrift eftersom handskriven text som skrivs på en skrivyta med positionskodningsmönster kan registreras elektroniskt som en sekvens av koordinater genom fortlöpande avläsning av positionskodningsmönstret. Positionskodningsmönster som kan användas för registrering av handskriven text beskrivs i exempelvis US 5,852,434 och i sökandens svenska patentansökningar SE 9901954-9 och SE 99003541-2, som ingavs den 28 maj 1999 respektive 1 oktober 1999 och som således inte var offentliga vid ingivande av föreliggande ansökan. Åtminstone de i sökandens patentansökningar beskrivna positionskodningsmönstren kan koda koordinater för ett mycket stort antal positioner på en imaginär yta. Man kan då tilldela olika användare olika koordinatområden och avbilda positionskodningsmönstret som motsvarar koordinatområdet på ett personligt kort eller liknande som tilldelas användaren. Endast genom att läsa av koordinater från detta kort kan han komma åt en viss åtkomstskyddad enhet.

Den åtkomstskyddade enheten är en enhet som ska skyddas från obehöriga. Exempel på åtkomstskyddade enheter är datorer, byggnader, fordon, websidor och olika typer av elektronisk utrustning.

I en utföringsform av systemet enligt uppfinningen är kontrollorganen alltså anordnade att för kontrollen av användarens behörighet kontrollera om koordinaterna ligger inom ett förutbestämt koordinatområde.

Som ett mycket enkelt exempel kan man tänka sig en handhållen scanner eller digital penna för elektronisk registrering av handskrift där ägaren endast kan logga in genom att registrera koordinater från ett kort som han har fått vid köpet av scannern/pennan. I detta fall finns kontrollorganen i scannern/pennan och behöver bara ha information om omfattningen av det förutbestämda koordinatområdet och kontrollera att de registrerade koordinaterna ligger inom detta område.

Inloggning på olika exemplar av scannern/pennan kan kräva koordinater från olika koordinatområden.

Koordinatområdet definieras i förväg och kan exempelvis definieras som liggande innanför bestämda koordinater som representerar hörnen till området.

I en fördelaktig utföringsform av systemet är användarenheten anordnad att registrera en användarsignatur som en sekvens av koordinater som beskriver användarenhetens förflyttning när en användare skriver användarsignaturen med användarenheten och varvid nämnda minst två koordinater innefattar sekvensen av koordinater.

En fördel med att användaren skriver sin signatur är att säkerheten ökar. Signaturen är vanligtvis användarens namnteckning, men kan också vara en symbol eller någon typ av tecken. För att en obehörig skall kunna logga in på den åtkomstskyddade enheten krävs alltså i detta fall både tillgång till den behörige användarens koordinatområde och signatur. Denna högre säkerhet kan implementeras utan att systemets hårdvara behöver ändras eftersom signaturregistreringen och koordinatregistreringen kan ske med samma teknik.

Kontrollorganen är lämpligen anordnade att jämföra sekvensen av koordinater, som alltså representerar den registrerade signaturen, med en tidigare lagrad sekvens av koordinater för kontrollen av användarens behörighet. Endast om sekvenserna överensstämmer i önskad utsträckning ges klarsignalen till den åtkomstskyddade enheten.

Användarenheten, kontrollorganen och den åtkomstskyddade enheten kan vara fysiskt placerade på olika sätt i förhållande till varandra.

Kontrollorganen kan vara fysiskt integrerade med användarenheten, med den åtkomstskyddade enheten eller fristående. Kontrollorganen kan också vara fysiskt uppdelade, vilket innebär att viss del av behörighetskontrollen sker på ett ställe och en annan del av behörighetskontrollen sker på ett annat ställe. Exempelvis kan en första kontroll ske i användarenheten och en andra kontroll i den åtkomstskyddade enheten.

När kontrollorganen är fristående kan de användas gemensamt för ett flertal användarenheter och ett flertal åtkomstskyddade enheter. De blir då mera komplicerade och behöver bl a ha större minnes- och bearbetningskapacitet.

När kontrollorganen är integrerade med användarenheten behöver de bara kunna kontrollera användare av den eller de åtkomstskyddade enheter som kan åtkommas via användarenheten.

I en utföringsform av systemet är den åtkomstskyddade enheten integrerad med användarenheten.

Åtkomsten gäller då själva användarenheten, varvid användarenheten och den åtkomstskyddade enheten kan ses som en och samma enhet. I detta fall startar användaren enheten och måste då göra en inloggning, vid vilken han endast kan använda de funktioner hos enheten som krävs för inloggningen, dvs registrering av koordinater och eventuella andra inloggningsparametrar. De funktioner som är tillgängliga vid inloggningen kan sägas motsvara användarenheten, medan övriga funktioner som blir tillgängliga först efter korrekt inloggning kan sägas motsvara den åtkomstskyddade enheten.

Kontrollorganen kan, men behöver inte vara, integrerade med användarenheten och den åtkomstskyddade enheten.

Den åtkomstskyddade enheten kan alternativt vara fristående från användarenheten. Den kan vara integrerad med kontrollorganen.

I en fördelaktig utföringsform av systemet är den åtkomstskyddade enheten en digital penna, som kan användas för digitalisering av handskriven text.

Såsom redan nämnts kan kontrollorganen vara gemensamma för flera användarenheter, som skickar de registrerade koordinaterna till kontrollorganen. I denna utföringsform av systemet finns det i kontrollorganen lagrat uppgifter om ett flertal koordinatområden. Kontrollorganen kan exempelvis vara webbaserade och nås via ett datornätverk.

Varje koordinatområde kan associeras med en eller flera användare och/eller en eller flera åtkomstskyddade enheter. I det förra fallet kan alltså flera användare komma åt en enhet genom registrering av koordinater från ett och samma förutbestämda område. Detta kan exempelvis vara önskvärt om den åtkomstskyddade enheten är en dator som flera personer skall kunna använda eller en lokal som flera personer skall kunna få tillträde till. I det senare fallet kan exempelvis en person komma åt olika åtkomstskyddade enheter genom registrering av koordinater från ett och samma förutbestämda koordinatområde. En person kan exempelvis vilja kunna logga in till olika apparater via ett standardinloggningsförfarande.

I en utföringsform av systemet är den åtkomstskyddade enheten associerad med minst ett av nämnda flertal koordinatområden.

Koordinaterna som registreras av användarenheten styr vilken åtkomstskyddad enhet som åtkomsten avser. Detta medför ett enkelt och smidigt sätt att få åtkomst till en bestämd åtkomstskyddad enhet. Olika koordinatområden kan associeras med olika åtkomstskyddade enheter. Ett koordinatområde kan också associeras med mer än en åtkomstskyddad enhet, men då måste användaren på något

sätt indikera vilken åtkomstskyddad enhet som han önskar komma åt.

I en utföringsform av systemet finns det med minst ett av nämnda flertal koordinatområden associerat minst en behörig användaridentitet.

Koordinaterna som registreras av användarenheten styr här användaridentiteten. Inom koordinatområdet som associeras med minst en behörig användare kan också finnas delområden som associeras med olika åtkomstskyddade enheter. Fördelen med detta är att om någon kan förfalska en signatur måste han också ha tillgång till underlaget med de bestämda koordinaterna som associeras med signaturen.

I en utföringsform innefattar systemet ett underlag, vilket är försett med ett positionskodningsmönster, som möjliggör bestämning av koordinater och från vilket användarenheten är anordnad att registrera nämnda minst två koordinater.

Beroende på var på underlaget användaren sätter ned användarenheten registreras olika koordinater. Koordinaterna kan tilldelas olika betydelser. Underlaget kan delas in i olika koordinatområde i vilka användaren skriver sin signatur eller bara sätter användarenheten mot. Beroende på vilket koordinatområde användaren väljer kan exempelvis åtkomst till olika enheter ske. Detta medför en för användaren snabb och smidig aktivering av den åtkomstskyddade enheten.

I en utföringsform innefattar användarenheten en optisk sensor och bildbehandlingsorgan för registrering av nämnda minst två koordinater.

Den optiska sensorn upptar bilder och bildbehandlingsorgan behandlar bilderna, vilket innefattar att bestämma koordinaterna utifrån innehållet i bilderna, varvid innehållet kan vara ovannämnda positionskodningsmönster.

Uppfinningen avser vidare enligt en andra aspekt en kontrollanordning för kontroll av en användares åtkomst

av en åtkomstskyddad enhet, varvid det i kontrollanordningen finns lagrat uppgifter om minst ett koordinatområde, varvid kontrollanordningen är anordnad att mottaga minst två koordinater från en användarenhet, som tillhör användaren, att kontrollera, på basis av de mottagna koordinaterna, om användaren är behörig att komma åt den åtkomstskyddade enheten och att om så är fallet avge en klarsignal till en åtkomstskyddad enhet.

Fördelen med kontrollanordningen framgår av diskussionen ovan av systemet och dess kontrollorgan.

Uppfinningen avser också enligt en tredje aspekt ett sätt att med hjälp av en användarenhet styra åtkomst till en åtkomstskyddad enhet, innefattande stegen att med användarenheten registrera minst två koordinater från ett underlag, att med kontrollorgan och på basis av de registrerade koordinaterna kontrollera om användaren är behörig att komma åt den åtkomstskyddade enheten, och att om så är fallet avge en klarsignal till den åtkomstskyddade enheten.

Enligt en fjärde aspekt av uppfinningen avser denna ett datorprogram som är lagrat på ett minnesmedium som kan avläsas av en dator och som innefattar instruktioner för att bringa datorn att utföra ett sätt enligt något av krav 23-29.

Enligt en femte aspekt avser uppfinningen en användning av ett positionskodningsmönster som kodar koordinater för att styra åtkomst till en åtkomstskyddad enhet.

Fördelarna med sättet, datorprogrammet och användningen framgår av diskussionen ovan. De särdrag som diskuterats angående systemet gäller också i tillämpliga delar för kontrollanordningen, sättet, datorprogrammet och användningen.

Kort beskrivning av ritningarna

Uppfinningen kommer att beskrivas närmare i det följande genom utföringsexempel och under hänvisning till bifogade ritningar, på vilka

Fig 1 visar ett system enligt en första utföringsform av föreliggande uppfinning, vilket system innefattar en digital penna och ett koordinatunderlag.

Fig 2 visar ett exempel på en andra utföringsform av ett system enligt uppfinningen, vilket system innefattar en användarenhet och ett inloggningskort.

Fig 3 visar schematiskt ett exempel på en lagringsstruktur för lagring av bland annat kontrollinformation i en kontrollanordning som används i ett system enligt uppfinningen.

Beskrivning av föredragna utföringsformer

I det följande ges två exempel på hur uppfinningen kan realiseras. Det första exemplet avser åtkomst av en digital penna. Det andra exemplet avser åtkomst av en dator. I det första exemplet är hela systemet för styrning av åtkomst av den digitala pennan integrerat med den digitala pennan. I det andra exemplet är systemet för åtkomststyrning separerat från den åtkomstskyddade enheten, dvs datorn.

I fig 1 visas en digital penna 1 och ett koordinatunderlag 5. Den digitala pennan 1 kan användas som en vanlig penna, med den skillnaden att texten som skrivs kan erhållas i digital form i pennan. För att skydda pennan från obehöriga användare är denna försedd med ett system för styrning av åtkomst av den (ett inloggningssystem).

Inloggningskort

I fig 1 visas ett exempel på ett inloggningskort 5 som i detta fall till storlek och material liknar ett vanligt magnetkort. Inloggningskortet 5 har ett skrivområde 6 som är försett med koordinater, som kan avläsas av den digitala pennan 1. Koordinaterna kan vara angivna i explicit eller kodad form. I detta exempel är inloggningskortet 5 försett med koordinater som är kodade med hjälp av ett positionskodningsmönster 7. Mönstret 7 visas schematiskt som ett antal prickar på en del av inloggningskortet 5.

Skrivområdet 6 är avsett för användarens signatur. Inloggningskortet kan vara utformat av sådant material så att signaturen kan suddas ut efter att ha skrivits. Alternativt kan kombinationen av penna och inloggningskort vara sådan att inget färgämne avsätts på inloggningskortet när användaren skriver signaturen.

Positionskodningsmönstret 7 har egenskapen att om man registrerar en godtycklig del av mönstret med en viss minsta storlek så kan dennas position i positionskodningsmönstret och därmed inloggningskortet 5 bestämmas entydigt.

Positionskodningsmönstret 7 kan vara av sådan typ som visas i US 5,852,434, där varje position kodas av en specifik symbol.

Positionskodningsmönstret 7 är dock med fördel av den typ som visas i sökandens ovannämnda ansökningar SE 9901954-9 och SE 9903541-2, där varje position kodas av ett flertal symboler och varje symbol bidrar till kodningen av flera positioner. Positionskodningsmönstret 7 byggs upp av ett fåtal typer av symboler. Ett exempel visas i SE 9901954-9 där en större prick representerar en "etta" och en mindre prick representerar en "nolla". Ett annat exempel visas i SE 9901954-9, där fyra olika förskjutningar av en prick i förhållande till en rasterpunkt kodar fyra olika värden.

Digital penna

Den digitala pennan 1 i fig 1 innefattar ett hölje 11. I höljets kortända finns en öppning 12.

Höljet inrymmer i huvudsak en optikdel, en elektronikdel och en strömförsörjning.

Optikdelen innefattar minst en lysdiod 13 för belysning av den yta som skall avbildas och en ljuskänslig areasensor 14, exempelvis en CCD- eller CMOS-sensor, för registrering av en tvådimensionell bild. Eventuellt kan pennan dessutom innehålla ett linssystem.

Strömförsörjningen till pennan erhålls från ett batteri 15 som är monterat i ett separat fack i höljet 11.

Elektronikdelen innehåller en processor 16 som är programmerad till att läsa in en bild från sensorn 14, identifiera symboler i bilden, bestämma vilka två koordinater som symbolerna kodar och att lagra dessa koordinater i sitt minne. Processorn 16 är vidare programmerad till att analysera lagrade koordinatpar och omvandla dessa till ett polygontåg som utgör en beskrivning av hur användarenheten har förflyttats över en yta som är försedd med positionskodningsmönstret, vilken förflyttning exempelvis kan representera användarens signatur eller någon annan form av handskriven information.

Pennan 1 innefattar vidare en pennspets 17, med vars hjälp användaren kan skriva vanlig färgämnesbaserad skrift som samtidigt som den skrivs registreras digitalt av pennan 1 med hjälp av positionskodningsmönstret. Pennspetsen 17 är in- och utfällbar så att användaren kan styra om den skall användas eller ej.

Pennan 1 innefattar vidare knappar 18 med vars hjälp enheten aktiveras och styrs. Den har också en sändtagare 19 för trådlös kommunikation, t ex med IR-ljus eller radiovågor, med externa enheter.

Inloggning med hjälp av pennan

Såsom nämnts är pennan 1 försedd med ett inloggningssystem. När pennan slås på måste användaren logga in för att kunna använda den. För hantering av inloggningen är pennan 1 försedd med ett inloggningsprogram. Dessutom finns i minnet lagrat information åtminstone om användarens specifika koordinatområde.

I ett första exempel är åtkomstenheten den digitala pennan 1, vilken också innefattar kontrollorganen som innefattar ett minne i vilket finns lagrat koordinatområden och tillhörande användaridentiteter. Flera användare kan ha behörighet till pennan 1. Varje användare kan ha sitt inloggningskort 5. Inloggningskortet 5 kan vara

ett kort som användaren bär med sig exempelvis i sin plånbok. Då en användare önskar logga in på den digitala pennan 1 sätter hon den mot inloggningskortets 5 skrivområde 6, som är försett med ett för användaren unikt positionskodningsmönster 7. En del av mönstret läses in optiskt av den digitala pennan 1. Ett program omvandlar mönstret till koordinater som överförs till kontrollorganen. Kontrollorganen kontrollerar att koordinaterna ligger innanför ett förutbestämt koordinatområde tillhörande en behörig användare. Om så är fallet får användaren åtkomst till den digitala pennans 1 funktioner. Olika användare har olika koordinatområde, vilket medför att man kan styra vilka program som olika användare ska kunna få tillgång till genom att pennan startar olika program beroende på i vilket koordinatområde de registrerade koordinater hamnar. För att öka säkerheten vid inloggning ytterligare kan det av en användare krävas att hon ska skriva in sin signatur på skrivområdet. Signaturen överförs till kontrollorganen som en sekvens av koordinater. Kontrollorganen kontrollerar, förutom inom vilket område koordinaterna ligger, även om sekvensen av koordinater för detta koordinatområde överensstämmer med en i minnet lagrad behörig sekvens. Det räcker nu inte att en obehörig kommer över skrivunderlaget och pennan, utan den obehörige måste också kunna förfalska den behörige användarens signatur för att få åtkomst till pennans funktioner.

Inloggning till dator

I fig 2 visas en andra utföringsform av uppfinningen i vilken den åtkomstskyddade enheten en dator 4, användarenheten är en digital penna 1 och kontrollorganen finns på webben i form av en serverenhet 2. Serverenheten 2 betjänar ett flera digitala pennor 1 och flera datorer 4.

Den digitala pennan 1 är anordnad att överföra information som genereras av användaren till serverenheten 2. I detta exempel överförs informationen trådlöst till

en nätverksanslutningsenhet 8, som i sin tur överför informationen till serverenheten 2. Nätverksanslutningsenheten 8 är i detta exempel en mobiltelefon. Den kan alternativt vara en dator eller någon annan lämplig enhet som har ett gränssnitt mot ett nätverk, exempelvis Internet eller ett lokalt företagsnät. Nätverksanslutningsenheten kan alternativt utgöra en integrerad del av användarenheten.

Serverenheten 2 är en dator i ett nätverk av datorer. Den är uppbyggd som en traditionell serverenhet med en eller flera processorer, minne av olika slag, periferienheter och kopplingar till andra datorer i nätverket, men den har ny programvara för att utföra de här beskrivna funktionerna. Den har också information lagrad i sitt minne för att kunna hantera dessa funktioner.

I serverenhetens 2 minne finns lagrad information om koordinatområden. Koordinatområdena kan vara olika stora och ha olika form. Ett rektangulärt koordinatområde kan exempelvis vara beskrivet med hjälp av koordinatpar som representerar punkterna i hörnen på koordinatområdet. Skrivområdet 6 på inloggningskortet 5 upptar ett koordinatområde.

I en datastruktur i serverenhetens 2 minne finns uppgifter eller regler för varje koordinatområde som definierar hur informationen som kan tillordnas koordinatområdet skall behandlas.

I fig 3 visas ett exempel på en sådan struktur, som här utgörs av en tabell. I en första kolumn 30 i tabellen definieras koordinatområdena med hjälp av koordinaterna (x1,y1; x2,y2; x3,y3; x4,y4) för hörnen på koordinatområdet som här antas vara rektangulära. I en andra kolumnen 31 finns en representation av den behörige användarens signatur lagrad så att serverenheten 2 kan jämföra en mottagen signatur med en tidigare lagrade signaturen. I en tredje kolumn 32 är en användaridentitet lagrad i form av ett serienummer för den behörige användarens användarenhet 1. Naturligtvis är detta en mycket enkel

struktur som bara används för att illustrera principerna. Betydligt mera komplexa strukturer och regler för säkerhetskontroll är tänkbara.

När en användare önskar få åtkomst till en dator 4 sätter hon den digitala pennan 1 mot skrivområdet 6 och pennan 1 registrerar mönstret 7 och räknar ut motsvarande koordinater. Koordinaterna skickas tillsammans med en i användarenheten 1 lagrad användaridentitet vidare via mobiltelefonen 8 till serverenheten 2. Serverenheten 2 kontrollerar till vilket koordinatområde de registrerade koordinaterna tillhör. Varje dator 4 i systemet associeras med minst ett koordinatområde. Serverenheten 2 avgör på så sätt vilken dator som åtkomsten avser. Serverenheten 2 kontrollerar sedan att användaridentiteten har behörighet att logga in på den dator som inloggningen avser. Om användaren har behörighet skickas en signal till den dator 4 som åtkomsten avser, vilket medför att användaren nu loggat in på datorn 4. Det är möjligt att skicka med speciell information från serverenheten till den berörda datorn 4. Denna speciella information kan innefatta användarspecifika uppgifter som exempelvis startar för användaren specifika program. Det kan också vara så att olika användare ska få åtkomst till olika mycket information på datorn 4, vilket innebär att endast vissa delar av datorns 4 innehåll öppnas upp för användaren. Om användaren ej har behörighet till datorn 4 kan ett meddelande om detta skickas till den digitala pennan 1.

För att öka säkerheten i detta system ytterligare skriver användaren sin signatur på inloggningskortets 5 skrivområde 6. Signaturen registreras som en sekvensen av koordinater och skickas tillsammans med det i användarenheten lagrade användaridentiteten, vidare via mobiltelefonen 8 till serverenheten 2. Serverenheten 2 jämför den mottagna sekvensen av koordinater, dvs signaturen, med en med användaridentiteten tidigare lagrad sekvens av koordinater. Om den mottagna signaturen bedöms överens-

stämma, skickas en signal till datorn 4 och användaren loggas in.

Det är också möjligt att anordna kontrollorganen i datorn 4, dvs den åtkomstskyddade enheten.

Engångskod

Ett förutbestämt koordinatområde på ett skrivunderlag kan också fungera som ett engångsområde, som efter att det använts en gång är förbrukat. Detta kan exempelvis vara användbart när man önskar kunna slänga skrivunderlaget efter användning eller när man önskar behålla det som en kvittens för åtkomst till systemet. Det kan vara så att namnskriften också skrivs på underlaget med bläck vilket medför att om en obehörig hittar lappen kan det vara relativt enkelt för honom att följa den skrivna namnskriften och på så sätt få åtkomst till den åtkomstskyddade enheten. Är däremot detta mönster förbrukat så blir den enda informationen användarens signatur.

Även om en speciella utföringsformer av uppfinningen har beskrivits ovan är det uppenbart för fackmannen att många alternativ, modifieringar och variationer är möjliga att åstadkomma i ljuset av ovanstående beskrivning.

PATENTKRAV

1. System för styrning av en användares åtkomst av en åtkomstskyddad enhet (4), k ä n n e t e c k n a t av att systemet innefattar en användarenhet (1), som är anordnad att registrera minst två koordinater, och kontrollorgan (2), som är anordnade att, på basis av nämnda två koordinater, kontrollera om användaren är behörig att komma åt den åtkomstskyddade enheten (4) och att om så är fallet avge en klarsignal till den åtkomstskyddade enheten (4).

2. System enligt krav 1, i vilket kontrollorganen (2) är anordnade att för kontrollen av användarens behörighet kontrollera om koordinaterna ligger inom ett förutbestämt koordinatområde.

3. System enligt krav 1 eller 2, varvid användarenheten (1) är anordnad att registrera en användarsignatur som en sekvens av koordinater som beskriver användarenhetens förflyttning när en användare skriver användarsignaturen med användarenheten (1) och varvid nämnda minst två koordinater innefattar sekvensen av koordinater.

4. System enligt krav 3, varvid kontrollorganen (2) är anordnade att jämföra sekvensen av koordinater med en tidigare lagrad sekvens av koordinater för kontrollen av användarens behörighet.

5. System enligt något av föregående krav, varvid kontrollorganen (2) är integrerade med användarenheten (1).

6. System enligt något av föregående krav, varvid den åtkomstskyddade enheten (4) är integrerad med användarenheten (1).

7. System enligt något av föregående krav, varvid den åtkomstskyddade enheten (4) är en digital penna.

8. System enligt något av föregående krav, varvid det i kontrollorganen (2) är lagrat uppgifter om ett flertal koordinatområden.

9. System enligt krav 8, varvid den åtkomstskyddade enheten (4) är associerad med minst ett av nämnda flertal koordinatområden.

10. System enligt krav 8 eller 9, varvid det med minst ett av nämnda flertal koordinatområden finns associerat minst en behörig användaridentitet.

11. System enligt något av föregående krav, vidare innefattande ett underlag (5), vilket är försett med ett positionskodningsmönster (7), som möjliggör beräkning av koordinater och från vilket användarenheten (1) är anordnad att registrera nämnda minst två koordinater.

12. System enligt något av föregående krav, varvid användarenheten (1) innefattar en optisk sensor och bildbehandlingsorgan för registrering av nämnda minst två koordinater.

13. Kontrollanordning (2) för kontroll av en användares åtkomst av en åtkomstskyddad enhet (4), k ä n n e t e c k n a t av att det i kontrollanordningen (2) finns lagrat uppgifter om minst ett koordinatområde, varvid kontrollanordningen (2) är anordnad att mottaga minst två koordinater från en användarenhet (1), som tillhör användaren, att kontrollera, på basis av de mottagna koordinaterna, om användaren är behörig att komma åt den åtkomstskyddade enheten (4) och att om så är fallet avge en klarsignal till den åtkomstskyddade enheten (4).

14. Kontrollanordning enligt krav 13, vidare anordnade att för kontrollen av användarens behörighet kontrollera om koordinaterna ligger inom ett förutbestämt koordinatområde.

15. Kontrollanordning enligt något av kraven 13-14, vidare anordnad att mottaga en sekvens av koordinater från en användarenhet (1), varvid nämnda minst två koordinater innefattar sekvensen av koordinater.

16. Kontrollanordning enligt krav 15, vidare anordnad att jämföra sekvensen av koordinater med en tidigare lagrad sekvens av koordinater för kontrollen av användarens behörighet.

17. Kontrollanordning enligt något av kraven 13-16, varvid kontrollanordningen (2) är integrerad med användarenheten (1).

18. Kontrollanordning enligt något av kraven 13-17, i vilken det finns lagrat uppgifter om ett flertal koordinatområden.

19. Kontrollanordning enligt krav 18, varvid den åtkomstskyddade enheten (4) är associerad med mer än ett av nämnda flertal koordinatområden.

20. Kontrollanordningen enligt krav 18 eller 19, varvid det med minst ett av nämnda flertal koordinatområden finns associerat minst en behörig användaridentitet.

21. Kontrollanordningen enligt något av kraven 14-19, vilken är en serverenhet (2).

22. Kontrollanordning enligt krav 21, varvid kommunikationen mellan användarenheten (1), kontrollanordningen (2) och den åtkomstskyddade enheten (4) sker via ett datornätverk (3).

23. Sätt att med hjälp av en användarenhet (1) styra åtkomst till en åtkomstskyddad enhet (4), innefattande stegen

att med användarenheten (1) registrera minst två koordinater från ett underlag (5),

att med kontrollorgan (2) kontrollera om användaren är behörig att komma åt den åtkomstskyddade enheten (4), och

att om så är fallet avge en klarsignal till den åtkomstskyddade enheten (4).

24. Sätt enligt krav 23, vidare innefattande steget att för kontrollen av användarens behörighet kontrollera om koordinaterna ligger inom ett förutbestämt koordinatområde.

25. Sätt enligt krav 23 eller 24, varvid steget att med användarenheten (1) registrera minst två koordinater innefattar steget att med användarenheten (1) registrera en sekvens av koordinater som beskriver användarenhetens (1) förflyttning när en användare skriver användarsignaturen med användarenheten (1).

26. Sätt enligt krav 25, vidare innefattande steget att jämföra sekvensen av koordinater med en tidigare lagrad sekvens av koordinater för kontroll av användarens behörighet.

27. Sätt enligt krav 24, vidare innefattande steget att avgöra vilket förutbestämt koordinatområde koordinaterna tillhör.

28. Sätt enligt krav 27, vidare innefattande steget att utifrån koordinatområdestillhörigheten avgöra vilken åtkomstskyddad enhet (4) som åtkomsten avser.

29. Sätt enligt krav 27 eller 28, vidare innefattande steget att utifrån koordinatområdestillhörigheten avgöra om användaren har behörighet till den åtkomstskyddad enheten (4) som åtkomsten avser.

30. Datorprogram som är lagrat på ett minnesmedium som kan avläsas av en dator och som innefattar instruktioner för att bringa datorn (4) att utföra något av sätten enligt kraven 23-29.

31. Användning av ett positionskodningsmönster (7), som möjliggör beräkning av koordinater, för att styra åtkomst till en åtkomstskyddad enhet (4).

SAMMANDRAG

Ett system för styrning av en användares åtkomst av en åtkomstskyddad enhet (4). Systemet innefattar en användarenhet (1), som är anordnad att registrera minst två koordinater, och kontrollorgan (2), som är anordnade att, på basis av koordinaterna, kontrollera om användaren är behörig att komma åt den åtkomstskyddade enheten (4). Om användaren är behörig är kontrollorganen anordnade att avge en klarsignal till den åtkomstskyddade enheten (4).

Publiceringsbild = Fig 2

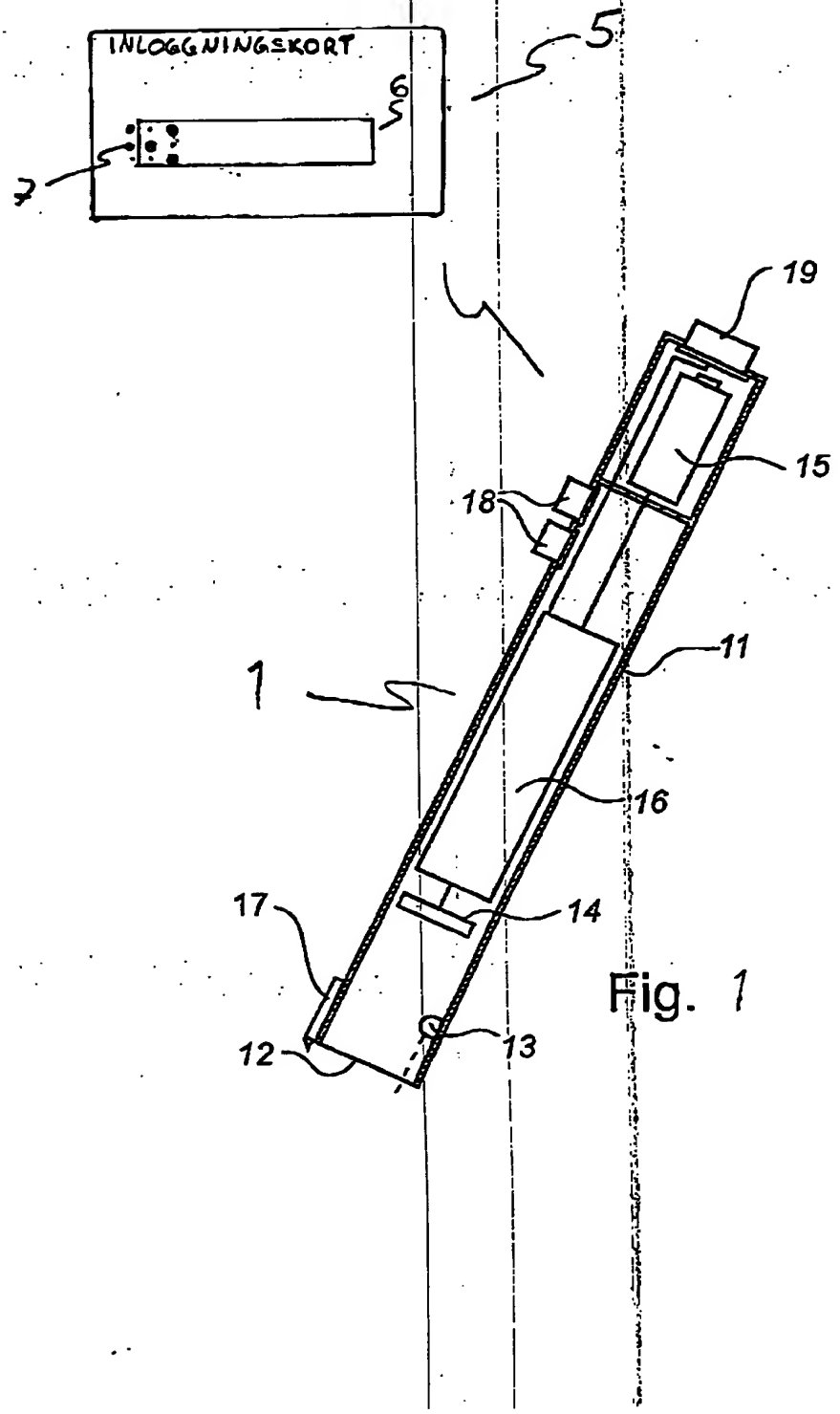

Fig. 1

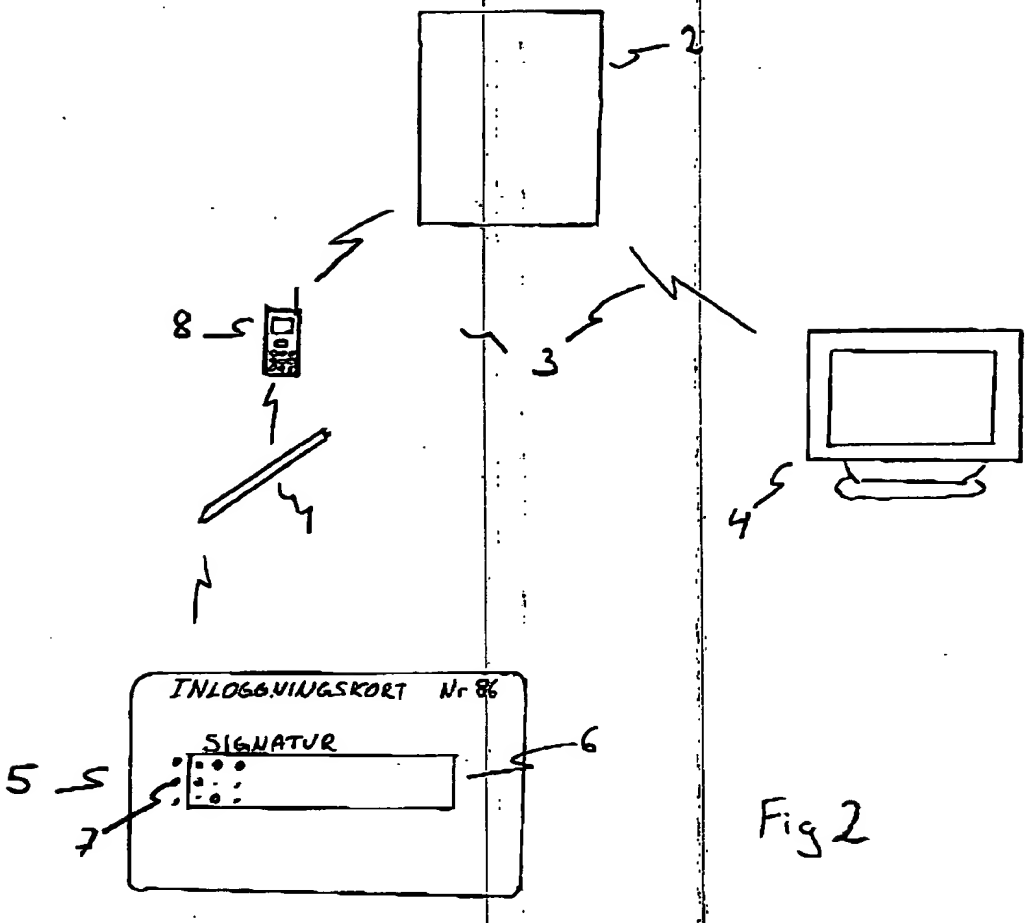

Fig 2

30 Koordinatområde	31 Signatur	32 Använd. ID
$(X_1Y_1);(X_2Y_2)$ $(X_3Y_3);(X_4Y_4)$	Per Rask	123 456

Fig 3